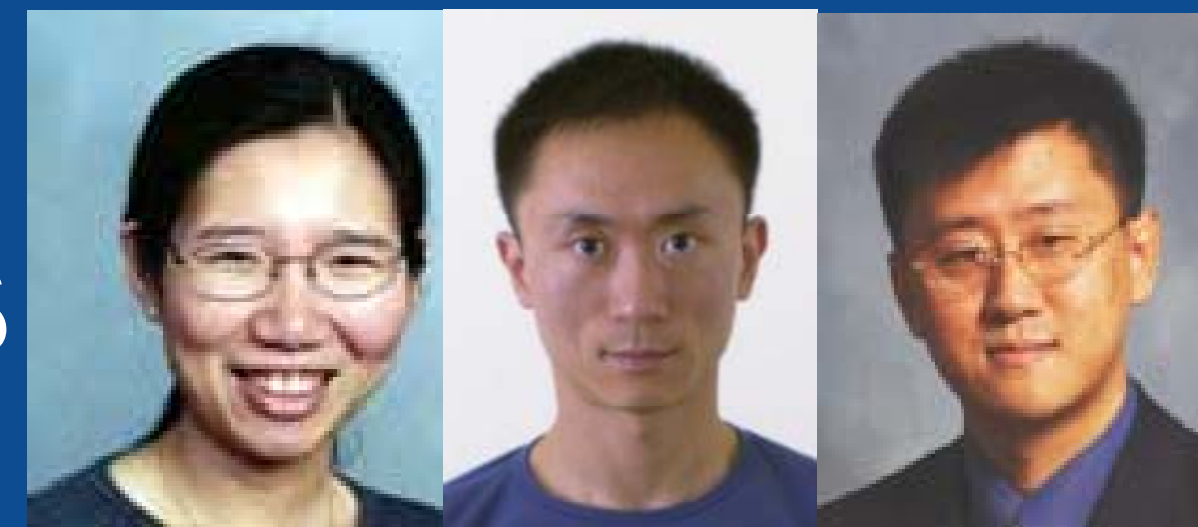


# Automatic Validation, Optimization, & Adaptation of Distributed Firewalls



Chen-Nee Chuah, Hao Chen, and Zhendong Su  
University of California, Davis

<http://www.ece.ucdavis.edu/rubinet/fireman.html>

## Project Goals

- Traffic-aware firewall configuration optimization
- Framework for evaluating heuristic optimization techniques

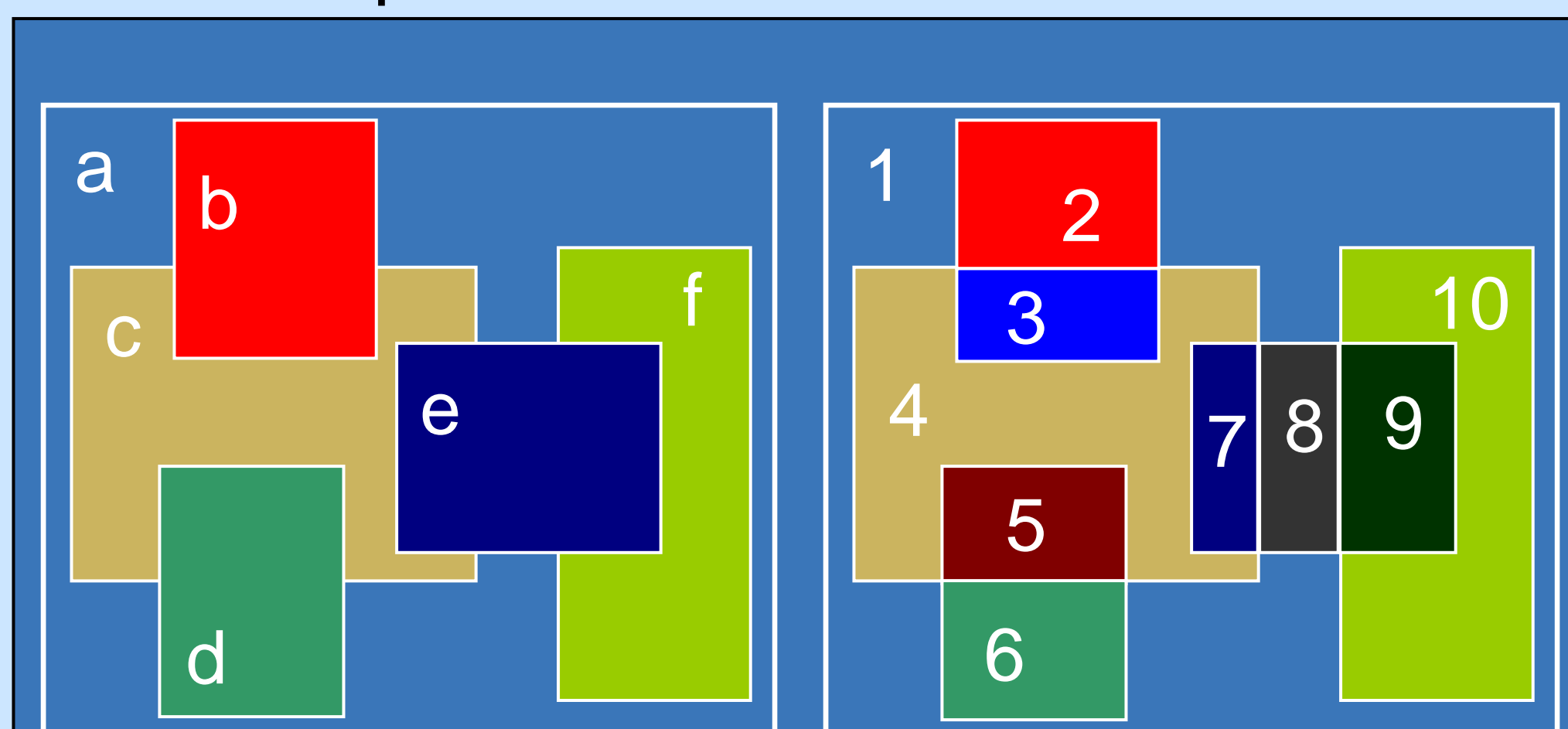
## Existing Challenges

- Dependency among rules
- Position-dependent rule weight

## Our Approach

### Dependency disentanglement

Find disjoint partitions with efficient set operations on rules. The weight of these partitions are not position-dependent.



With efficient set representation of firewall rules, FireOpt can effectively disentangle rules into disjoint partitions.

## Approach and Impact

### *New approach*

- Rule dependency disentanglement
- Partition-based traffic profile
- Partition-based ILP

### *Research Impact*

- Improved firewall performance
- Framework for evaluating ad hoc techniques

## Technical Discussion

Traffic-aware optimization for firewall configurations can improve the performance of existing firewalls with little cost. Several heuristics have been proposed but none of them can achieve the true optimality because of a.) over-conservative rule dependency constraint and b.) position-dependent.

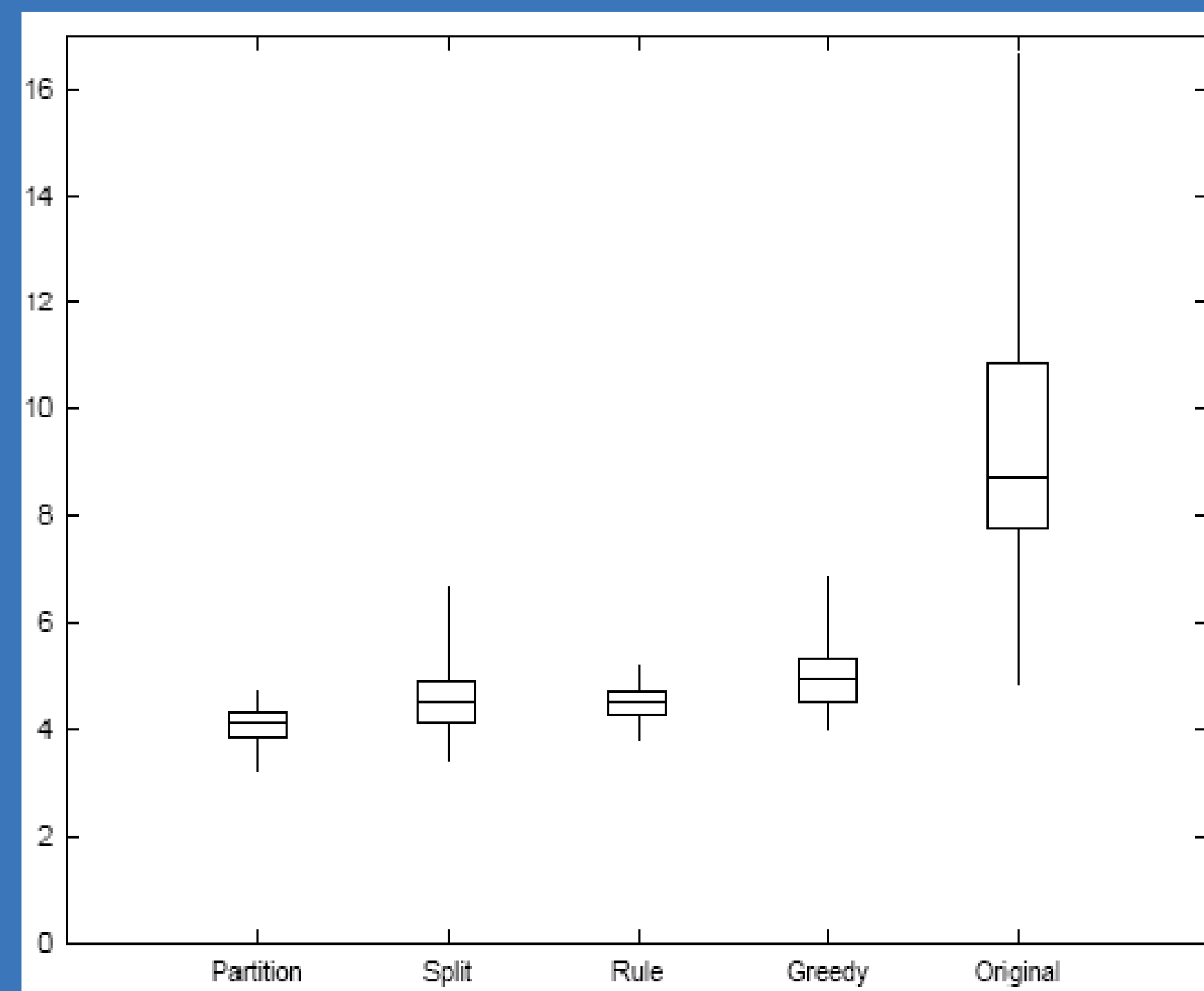
FireOpt presents an optimization framework that

1. Disentangle rules into disjoint partitions,
2. Measures partition-based traffic profile, and
3. Formulate an integer linear program.

FireOpt not only finds provable optimality but also provides a framework to evaluate other heuristics.

## Results

**FireOpt achieves provable optimality for rule-based configuration optimization.**



Cost Quartiles of various optimization techniques